日　本　国　特　許　庁 Masashi HAMADA
JAPAN PATENT OFFICE 4-26-01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年　５月　２日

出願番号
Application Number: 特願２０００－１３３４６９

出願人
Applicant(s): キヤノン株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　５月３０日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３０４６９５９

【書類名】　特許願

【整理番号】　3997006

【提出日】　平成12年 5月 2日

【あて先】　特許庁長官殿

【国際特許分類】　H04N　5/00

【発明の名称】　ユーザプロファイルの記憶方法、記憶装置、ユーザプロファイルの記憶媒体、情報端末装置及びプログラム格納した記憶媒体

【請求項の数】　26

【発明者】

【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

【氏名】　浜田　正志

【特許出願人】

【識別番号】　000001007

【氏名又は名称】　キヤノン株式会社

【代理人】

【識別番号】　100090273

【弁理士】

【氏名又は名称】　國分　孝悦

【電話番号】　03-3590-8901

【手数料の表示】

【予納台帳番号】　035493

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705348

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　ユーザプロファイルの記憶方法、記憶装置、ユーザプロファイルの記憶媒体、情報端末装置及びプログラム格納した記憶媒体

【特許請求の範囲】

【請求項１】　ユーザのプロファイルを記憶媒体に記憶するための個別ファイルを階層的に複数層分用意し、高レベルなセキュリティが要求されるユーザのプロファイルは深い階層の個別ファイルに記憶し、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルに記憶することを特徴とするユーザプロファイルの記憶方法。

【請求項２】　ユーザのプロファイルを記憶媒体に記憶するための個別ファイルを階層的に複数層分用意し、高レベルなセキュリティが要求されるユーザのプロファイルは認証処理が必要な個別ファイル、または認証処理が必要な個別ファイルの下層に記憶し、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルに記憶することを特徴とするユーザプロファイルの記憶方法。

【請求項３】　階層的に構成可能な個別ファイル内に存在する、少なくとも１つ以上の情報格納ファイル内に情報を記憶する方法であって、上記個別ファイル毎に独立した認証鍵を割り当てるようにユーザのプロファイルを記憶する方法において、

上記ユーザのプロファイルを記憶するための個別ファイルを上記記憶媒体に複数層分用意し、高レベルなセキュリティが要求されるユーザのプロファイルは深い階層の個別ファイルの情報格納ファイルに記憶するとともに、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルの情報格納ファイルに記憶することを特徴とするユーザプロファイルの記憶方法。

【請求項４】　上記積極的な提示が要求されるユーザのプロファイルが格納された個別ファイルには認証鍵を割当てず、自由なアクセスを可能にしたことを特徴とする請求項１～３の何れか１項に記載のユーザプロファイルの記憶方法。

【請求項５】　上記積極的な提示が要求されるユーザのプロファイルは、使用言語、要望する入出力インタフェース、それ以降の階層に認証処理を行うため

の情報、上記記憶媒体の所有者の基本情報であることを特徴とする請求項１～４の何れか１項に記載のユーザプロファイルの記憶方法。

【請求項６】　上記高度なセキュリティが必要なユーザのプロファイルは、ユーザの嗜好に関わる情報、同一記憶媒体内に存在する他の個別ファイルの認証鍵情報、上記記憶媒体の所有者のプライバシーに関わる情報であることを特徴とする請求項１～５の何れか１項に記載のユーザプロファイルの記憶方法。

【請求項７】　ユーザのプロファイルを記憶するための個別ファイルを記憶媒体に階層的に複数層分が用意されていて、高レベルなセキュリティが要求されるユーザのプロファイルは深い階層の個別ファイルに記憶され、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルに記憶されていることを特徴とするユーザプロファイルの記憶媒体。

【請求項８】　ユーザのプロファイルを記憶するための個別ファイルを記憶媒体に階層的に複数層分が用意されていて、高レベルなセキュリティが要求されるユーザのプロファイルは、認証処理が必要な個別ファイルか、または認証処理が必要な個別ファイルの下層に記憶され、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルに記憶されていることを特徴とするユーザプロファイルの記憶媒体。

【請求項９】　階層的に構成可能な個別ファイル内に存在する、少なくとも１つ以上の情報格納ファイル内に情報が記憶可能であり、上記個別ファイル毎に独立した認証鍵を割り当てることが可能な記憶媒体であって、

上記個別ファイルを複数層分用意し、高レベルなセキュリティが要求されるユーザのプロファイルは深い階層の個別ファイルの情報格納ファイルに記憶され、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルの情報格納ファイルに記憶されていることを特徴とするユーザプロファイルの記憶媒体。

【請求項１０】　上記積極的な提示が要求されるユーザのプロファイルが格納された個別ファイルには認証鍵を割当てず、自由なアクセスを可能にしたことを特徴とする請求項７～９の何れか１項に記載のユーザプロファイルの記憶媒体。

【請求項１１】　上記積極的な提示が要求されるユーザのプロファイルは、使用言語、要望する入出力インタフェース、これ以降の階層に認証処理を行うための情報、上記記憶媒体の所有者の基本情報であることを特徴とする請求項７～１０の何れか１項に記載のユーザプロファイルの記憶媒体。

【請求項１２】　上記高度なセキュリティが必要なユーザのプロファイルは、ユーザの嗜好に関わる情報、同一記憶媒体内に存在する他の個別ファイルの認証鍵情報、上記記憶媒体の所有者のプライバシーに関わる情報を含むことを特徴とする請求項７～１１の何れか１項に記載のユーザプロファイルの記憶媒体。

【請求項１３】　上記記憶媒体はＩＣカードであることを特徴とする請求項７～１２の何れか１項に記載のユーザプロファイルの記憶媒体。

【請求項１４】　上記記憶媒体は携帯端末であることを特徴とする請求項７～１２の何れか１項に記載のユーザプロファイルの記憶媒体。

【請求項１５】　上記請求項７～１４の何れか１項に記載のユーザプロファイルの記憶媒体とデータ通信を行うことが可能に構成されていることを特徴とする情報端末装置。

【請求項１６】　上記請求項７～１４の何れか１項に記載のユーザプロファイルの記憶媒体が装着された際に、上記ユーザプロファイルの記憶媒体に格納されている上記積極的な提示が要求されるユーザのプロファイル情報に従って、使用言語、入出力インタフェースを含む情報通信環境を、上記ユーザプロファイルの記憶媒体の所有者である利用者の所望の環境に変更することを特徴とする情報端末装置。

【請求項１７】　上記請求項７～１４の何れか１項に記載のユーザプロファイルの記憶媒体が装着された際に、上記ユーザプロファイルの記憶媒体に格納されている上記積極的な提示が要求されるユーザのプロファイル情報を利用して、利用者の同一性判定処理を実行することを特徴とする情報端末装置。

【請求項１８】　上記利用者の同一性判定処理の結果、現在の端末装置の利用者が正当なユーザであると判定した場合、上記高度なセキュリティが必要な個別ファイルへのアクセスを行うことを特徴とする請求項１７に記載の情報端末装置。

【請求項１９】　上記利用者の同一性判定処理の結果、現在の端末装置の利用者が不当なユーザであると判定した場合、上記高度なセキュリティが必要な個別ファイルへのアクセスは行わずに、今回の利用者の情報を上記記憶媒体に記憶するとともに、少なくともカード発行元及び警察を含む関係機関に通報することを特徴とする請求項１７に記載の情報端末装置。

【請求項２０】　ユーザのプロファイルを記憶媒体に記憶するための個別ファイルを階層的に複数層分用意し、高レベルなセキュリティが要求されるユーザのプロファイルは深い階層の個別ファイルに記憶し、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルに記憶する手段を具備することを特徴とするユーザプロファイルの記憶装置。

【請求項２１】　ユーザのプロファイルを記憶媒体に記憶するための個別ファイルを階層的に複数層分用意し、高レベルなセキュリティが要求されるユーザのプロファイルは認証処理が必要な個別ファイル、または認証処理が必要な個別ファイルの下層に記憶する手段と、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルに記憶する手段とを具備することを特徴とするユーザプロファイルの記憶装置。

【請求項２２】　階層的に構成可能な個別ファイル内に存在する、少なくとも１つ以上の情報格納ファイル内に情報を記憶する装置であって、上記個別ファイル毎に独立した認証鍵を割り当てるようにユーザのプロファイルを記憶する装置において、

上記ユーザのプロファイルを記憶するための個別ファイルを上記記憶媒体に複数層分用意し、高レベルなセキュリティが要求されるユーザのプロファイルは深い階層の個別ファイルの情報格納ファイルに記憶するとともに、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルの情報格納ファイルに記憶する手段を具備することを特徴とするユーザプロファイルの記憶装置。

【請求項２３】　上記積極的な提示が要求されるユーザのプロファイルが格納された個別ファイルには認証鍵を割当てず、自由なアクセスを可能にしたことを特徴とする請求項２０～２２の何れか１項に記載のユーザプロファイルの記憶装置。

【請求項２４】　上記積極的な提示が要求されるユーザのプロファイルは、使用言語、要望する入出力インタフェース、それ以降の階層に認証処理を行うための情報、上記記憶媒体の所有者の基本情報であることを特徴とする請求項２０～２３の何れか１項に記載のユーザプロファイルの記憶装置。

【請求項２５】　上記請求項１～６の何れか１項に記載のユーザプロファイルの記憶方法を実行するプログラムをコンピュータから読み出し可能に格納したことを特徴とする記憶媒体。

【請求項２６】　上記請求項２０～２４の何れか１項に記載のユーザプロファイルの記憶装置を構成するプログラムをコンピュータから読み出し可能に格納したことを特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はユーザプロファイルの記憶方法、記憶装置、ユーザプロファイルの記憶媒体、情報端末装置及びコンピュータから読み出し可能な記憶媒体に関し、特に、ＩＣカード等、階層的に構成可能な個別ファイル内に存在する、少なくとも１つ以上の情報格納ファイル内に情報が記憶可能であり、上記個別ファイル毎に独立した認証鍵を割当てることが可能な記憶媒体に用いて好適なものである。

【０００２】

【従来の技術】

従来、ユーザのプロファイルの記憶媒体として多く用いられていた磁気記憶媒体、光学記憶媒体は、階層的に構成可能な個別ファイル内に存在する、少なくとも１つ以上の情報格納ファイル内に情報が記憶可能であるが、上記個別ファイル毎に独立した認証鍵を割当てることが不可能であったため、ユーザのプロファイルは全て一元的に記憶して認証鍵を割当ることにより保護されていた。

【０００３】

【発明が解決しようとする課題】

しかしながら、上記の従来例では以下のような問題点があった。すなわち、従来の端末装置の場合には、ユーザのプロファイルを格納した記憶媒体が装着され

た際に、上記端末装置のユーザが初期認証処理を行うために必要な認証情報（パスワード等）を入力して初期認証処理に成功する前には、上記記憶媒体中のユーザのプロファイル情報を読み出すことができなかった。

【０００４】

このため、初期認証処理を行うための認証情報の入力手段を含む、初期ユーザインタフェースの選択は端末装置側に委ねられているので、ユーザの嗜好と相容れないインタフェースが選択されてしまう可能性があった。

【０００５】

例えば、ユーザは音声入力インタフェースを要望しているにもかかわらず、端末装置側はタッチパネルによる入力インタフェースを選択したりすることがあった。また、ユーザは使用言語として英語を要求しているにもかかわらず、端末装置側は日本語を使用言語と選択したりすることがあった。

【０００６】

すなわち、従来情報端末装置とユーザプロファイルの記憶媒体との間で情報を送受信する場合には、初期認証処理が行われる前は、ユーザのプロファイルに対応したユーザインタフェースの選択は、ユーザのプロファイルのセキュリティレベルを維持したまま実現することは不可能であった。

【０００７】

本発明は上述の問題点にかんがみ、高レベルなセキュリティが要求されるユーザのプロファイルを確実に保護した上で、ユーザが所望する入出力インタフェースを使用した情報の送受信を行うことができるようにすることを目的とする。

【０００８】

【課題を解決するための手段】

本発明のユーザプロファイルの記憶方法は、ユーザのプロファイルを記憶媒体に記憶するための個別ファイルを階層的に複数層分用意し、高レベルなセキュリティが要求されるユーザのプロファイルは深い階層の個別ファイルに記憶し、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルに記憶することを特徴としている。

また、本発明の他の特徴とするところは、ユーザのプロファイルを記憶媒体に

記憶するための個別ファイルを階層的に複数層分用意し、高レベルなセキュリティが要求されるユーザのプロファイルは認証処理が必要な個別ファイル、または認証処理が必要な個別ファイルの下層に記憶し、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルに記憶することを特徴としている。

また、本発明のその他の特徴とするところは、階層的に構成可能な個別ファイル内に存在する、少なくとも１つ以上の情報格納ファイル内に情報を記憶する方法であって、上記個別ファイル毎に独立した認証鍵を割り当てるようにユーザのプロファイルを記憶する方法において、上記ユーザのプロファイルを記憶するための個別ファイルを上記記憶媒体に複数層分用意し、高レベルなセキュリティが要求されるユーザのプロファイルは深い階層の個別ファイルの情報格納ファイルに記憶するとともに、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルの情報格納ファイルに記憶することを特徴としている。

また、本発明のその他の特徴とするところは、上記積極的な提示が要求されるユーザのプロファイルが格納された個別ファイルには認証鍵を割当てず、自由なアクセスを可能にしたことを特徴としている。

また、本発明のその他の特徴とするところは、上記積極的な提示が要求されるユーザのプロファイルは、使用言語、要望する入出力インタフェース、それ以降の階層に認証処理を行うための情報、上記記憶媒体の所有者の基本情報であることを特徴としている。

また、本発明のその他の特徴とするところは、上記高度なセキュリティが必要なユーザのプロファイルは、ユーザの嗜好に関わる情報、同一記憶媒体内に存在する他の個別ファイルの認証鍵情報、上記記憶媒体の所有者のプライバシーに関わる情報を含むことを特徴としている。

【０００９】

本発明のユーザプロファイルの記憶媒体は、ユーザのプロファイルを記憶するための個別ファイルを記憶媒体に階層的に複数層分が用意されていて、高レベルなセキュリティが要求されるユーザのプロファイルは深い階層の個別ファイルに記憶され、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルに記憶されていることを特徴としている。

また、本発明の他の特徴とするところは、ユーザのプロファイルを記憶するための個別ファイルを記憶媒体に階層的に複数層分が用意されていて、高レベルなセキュリティが要求されるユーザのプロファイルは、認証処理が必要な個別ファイルか、または認証処理が必要な個別ファイルの下層に記憶され、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルに記憶されていることを特徴としている。

また、本発明のその他の特徴とするところは、階層的に構成可能な個別ファイル内に存在する、少なくとも１つ以上の情報格納ファイル内に情報が記憶可能であり、上記個別ファイル毎に独立した認証鍵を割り当てることが可能な記憶媒体であって、上記個別ファイルを複数層分用意し、高レベルなセキュリティが要求されるユーザのプロファイルは深い階層の個別ファイルの情報格納ファイルに記憶され、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルの情報格納ファイルに記憶されていることを特徴としている。

また、本発明のその他の特徴とするところは、上記積極的な提示が要求されるユーザのプロファイルが格納された個別ファイルには認証鍵を割当てず、自由なアクセスを可能にしたことを特徴としている。

また、本発明のその他の特徴とするところは、上記積極的な提示が要求されるユーザのプロファイルは、使用言語、要望する入出力インタフェース、これ以降の階層に認証処理を行うための情報、上記記憶媒体の所有者の基本情報であることを特徴としている。

また、本発明のその他の特徴とするところは、上記高度なセキュリティが必要なユーザのプロファイルは、ユーザの嗜好に関わる情報、同一記憶媒体内に存在する他の個別ファイルの認証鍵情報、上記記憶媒体の所有者のプライバシーに関わる情報を含むことを特徴としている。

また、本発明のその他の特徴とするところは、上記記憶媒体はＩＣカードであることを特徴としている。

また、本発明のその他の特徴とするところは、上記記憶媒体は携帯端末であることを特徴としている。

【００１０】

本発明の情報端末装置は、上記に記載のユーザプロファイルの記憶媒体とデータ通信を行うことが可能に構成されていることを特徴としている。

また、本発明の他の特徴とするところは、上記の何れか１項に記載のユーザプロファイルの記憶媒体が装着された際に、上記ユーザプロファイルの記憶媒体に格納されている上記積極的な提示が要求されるユーザのプロファイル情報に従って、使用言語、入出力インタフェースを含む情報通信環境を、上記ユーザプロファイルの記憶媒体の所有者である利用者の所望の環境に変更することを特徴としている。

また、本発明のその他の特徴とするところは、上記の何れか１項に記載のユーザプロファイルの記憶媒体が装着された際に、上記ユーザプロファイルの記憶媒体に格納されている上記積極的な提示が要求されるユーザのプロファイル情報を利用して、利用者の同一性判定処理を実行することを特徴としている。

また、本発明のその他の特徴とするところは、上記利用者の同一性判定処理の結果、現在の端末装置の利用者が正当なユーザであると判定した場合、上記高度なセキュリティが必要な個別ファイルへのアクセスを行うことを特徴としている。

また、本発明のその他の特徴とするところは、上記利用者の同一性判定処理の結果、現在の端末装置の利用者が不当なユーザであると判定した場合、上記高度なセキュリティが必要な個別ファイルへのアクセスは行わずに、今回の利用者の情報を上記記憶媒体に記憶するとともに、少なくともカード発行元及び警察を含む関係機関に通報することを特徴としている。

【００１１】

本発明のユーザプロファイルの記憶装置は、ユーザのプロファイルを記憶媒体に記憶するための個別ファイルを階層的に複数層分用意し、高レベルなセキュリティが要求されるユーザのプロファイルは深い階層の個別ファイルに記憶し、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルに記憶する手段を具備することを特徴としている。

また、本発明の他の特徴とするところは、ユーザのプロファイルを記憶媒体に記憶するための個別ファイルを階層的に複数層分用意し、高レベルなセキュリテ

ィが要求されるユーザのプロファイルは認証処理が必要な個別ファイル、または認証処理が必要な個別ファイルの下層に記憶する手段と、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルに記憶する手段とを具備することを特徴としている。

また、本発明のその他の特徴とするところは、階層的に構成可能な個別ファイル内に存在する、少なくとも１つ以上の情報格納ファイル内に情報を記憶する装置であって、上記個別ファイル毎に独立した認証鍵を割り当てるようにユーザのプロファイルを記憶する装置において、上記ユーザのプロファイルを記憶するための個別ファイルを上記記憶媒体に複数層分用意し、高レベルなセキュリティが要求されるユーザのプロファイルは深い階層の個別ファイルの情報格納ファイルに記憶するとともに、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルの情報格納ファイルに記憶する手段を具備することを特徴としている。

また、本発明のその他の特徴とするところは、上記積極的な提示が要求されるユーザのプロファイルが格納された個別ファイルには認証鍵を割当てず、自由なアクセスを可能にしたことを特徴としている。

また、本発明のその他の特徴とするところは、上記積極的な提示が要求されるユーザのプロファイルは、使用言語、要望する入出力インタフェース、それ以降の階層に認証処理を行うための情報、上記記憶媒体の所有者の基本情報であることを特徴としている。

【００１２】

本発明の記憶媒体は、上記の何れか１項に記載のユーザプロファイルの記憶方法を実行するプログラムをコンピュータから読み出し可能に格納したことを特徴としている。

【００１３】

本発明は上記技術手段を有するので、高レベルなセキュリティが要求されるユーザのプロファイルは容易に読み出されないように深い階層の個別ファイルに記憶され、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルに記憶されることにより、ユーザインタフェースや使用言語等等のように、

積極的な提示が要求されるユーザのプロファイルは、初期認証の成功前に端末装置側から読み出すことが可能となり、初期認証の成功以前から、ユーザ所望の入出力インタフェースでの動作が可能となり、しかも高レベルなセキュリティが要求されるユーザのプロファイルのセキュリティを高レベルに確保することが可能となる。

【００１４】

【発明の実施の形態】

（第１の実施形態）

本発明のユーザのプロファイルのユーザプロファイルの記憶方法、ユーザプロファイルの記憶媒体、情報端末装置及びコンピュータから読み出し可能な記憶媒体の一実施形態として、自治体等にて用いられる公共情報端末にスマートカード（ＩＣカード）を利用する例を示す。

【００１５】

図１は、本実施形態のシステム概念図である。図１において、１１が本実施形態のユーザのプロファイルの階層的な記憶媒体であるスマートカードであり、１２は上記記憶媒体１１を収容する対応端末である公共情報端末、１３が上記公共情報端末１２と各自治体のホスト（１４）との接続を司るネットワークである。上記公共情報端末１２にて、利用ユーザのプロファイルに応じた入出力手段の選択、トップメニューのカスタマイズ化等を容易に実現するのが、本実施形態の目的である。

【００１６】

図２は、本実施形態におけるスマートカード１１上の論理ファイル構造の一例を示す図である。

図２に示したように、ＭＦ（マスターファイル）２００の下に、スマートカード１１に実装されるアプリケーションファイルが設けられている。図２の例では、利用者認証、医療、電子マネー毎にＤＦ（デディケイティトファイル）２１０，２２０，２３０が設けられている。

【００１７】

上記利用者認証用のデディケイティトファイルＤＦ（２１０）の下に、カード

加入者の使用言語や要望入出力インタフェース、必要に応じて指紋や顔の特徴の量子化情報といったユーザ認証のためのカード所有者基本情報を格納するためのＥＦ（エレメンタリーファイル）２１１と端末利用者とが、スマートカード１１の加入者の場合に限ってアクセスを許容するセキュリティ情報格納ＢＯＸアプリケーション用のデディケイティトファイルＤＦ（２１２）を設け、この下のエレメンタリーファイルＥＦ（２１３～２１５）に、ユーザの嗜好や他のアプリケーション利用のための鍵情報といったセキュリティレベルの高い情報を格納する。

【００１８】

また、上記浅い階層に設けられている、利用者認証用のデディケイティトファイルＤＦ（２１０）のアクセス鍵に関しては一義的な鍵（システムに一意的な値）を割当てることにより、上記スマートカード１１が対応端末機器１２に装着された際には、セキュリティキーを格納しているエレメンタリーファイルＥＦ２０１の情報に加えて、セキュリティレベル「０」のユーザ情報として、カード加入者の使用言語や要望入出力インタフェース、必要に応じて指紋や顔の特徴の量子化情報といった、ユーザ認証のためのカード所有者の基本情報を格納するためのエレメンタリーファイルＥＦ（２１１）を読み出すことを可能な構成としている。

【００１９】

端末利用者が、スマートカード１１の加入者の場合に限ってアクセスを許容する。そして、セキュリティ情報格納ＢＯＸアプリケーション用のデディケイティトファイルＤＦ（２１２）をアクセスするために必要な鍵は、初期ユーザ認証処理の成功時に入手させる。これにより、セキュリティ情報格納ＢＯＸアプリケーション内の情報のセキュリティレベルを担保することができる。

【００２０】

上記ＤＦ（デディケイティトファイル）２２０は、医療系の情報を格納するものであり、この下の層に電子カルテアプリケーション用個別ファイル２２２、エレメンタリーファイルＥＦ２２１、電子カルテアプリケーション用情報ファイル２２３、電子カルテアプリケーション用情報ファイル（病歴）２２４が設けられている。

【００２１】

また、ＤＦ（デディケイティトファイル）２３０は電子マネー系アプリケーション用個別ファイルであり、この下の層に電子マネーアプリケーション用情報ファイル（取り引き履歴）２３１、電子マネーアプリケーション用情報ファイル（残高）２３２等が設けられている。

【００２２】

図３は、本実施形態システムの公共情報端末１２に対してスマートカード１１を装着した時に、端末利用者確認処理に成功した際のシーケンス例を示す図である。また、図４は、本実施形態システムの公共情報端末１２へのスマートカード１１を挿入した時に、端末利用者確認処理に失敗した際のシーケンス例を示す図である。これらの図３及び図４に示した処理を、図５のフローチャートを参照しながら説明する。

【００２３】

図５に、上記公共情報端末１２にスマートカード１１を装着した時に行われる処理手順の一例のフローチャートを示している。

先ず、最初のステップＳ５０１において、利用者認証アプリケーションが格納されている利用者認証用のデディケイティトファイルＤＦ２１０の選択処理（図３の３０１及び３０２、図４の４０１及び４０２）を行い、カード所有者基礎情報用のエレメンタリーファイルＥＦ２１１にアクセスして、利用者が所望する入出力Ｉ／Ｆ情報を読み出す（図３の３０３及び３０４、図４の４０３及び４０４）。

【００２４】

次に、ステップＳ５０２に進み、これに対応した入出力Ｉ／Ｆを選択して設定する（図３の３０３及び３０４、図４の４０３及び４０４）。その後、ステップＳ５０３に進んで、利用者が所望するインタフェースを用いて利用者認証処理を実行する。これは、上記認証手法に従って上記公共情報端末１２を利用する利用者と、上記スマートカード１１の所有者との同一性を確認する処理である（図３の３０５及び３０６、図４の４０５及び４０６）である。

【００２５】

次に、ステップＳ５０４において、上記ステップＳ５０３で実行した認証処理の結果に、スマートカード１１の所有者と公共情報端末１２の利用者とが一致しているか否かを判断する。

【００２６】

ステップＳ５０４の判断の結果、カード所有者と端末利用者とが一致しているのであれば、ステップＳ５０５に進み、セキュリティ情報ＢＯＸアプリケーションであるデディケイティトファイルＤＦ（２１２）へのアクセスを許容する。

【００２７】

次に、ステップＳ５０６に進み、セキュリティ情報ＢＯＸアプリケーションであるデディケイティトファイルＤＦ（２１２）との間でユーザ認証処理（図３の３０７）を行い、スマートカード１１内に格納されている他のデディケイティトファイルＤＦ用のパスワードを要求する（図３の３０８）。そして、それに応答して上記スマートカード１１から各アプリケーションパスワードを読み出し（図３の３０９）、許容サービスに応じた情報アクセスを行う。

【００２８】

一方、上記ステップＳ５０４の判断の結果、カード所有者と端末利用者が一致しないのであれは、ステップＳ５０７に進み、セキュリティ情報ＢＯＸアプリケーション用のデディケイティトファイルＤＦ（２１２）へのアクセスを禁止する。

【００２９】

次に、ステップＳ５０８に進み、カード利用者が不一致の際の各種セキュリティ処理を自律的に起動（４０７）する。これは、サービス機能制限、カード発行元への自動通報、端末利用者情報の記録、及び警察への通報等を行う処理である。

【００３０】

本実施形態においては、上述のような処理を順次実行することにより、公共情報端末１２を利用する際に、初期認証用の情報入力前に、上記公共情報端末１２を利用する者が所望する入出力インタフェースを上記公共情報端末１２側に認識させることが可能となる。

【００３１】

これにより、利用者が所望する入出力インタフェースを使用して情報システムを動作させることができ、所望のユーザ認証手段で、利用者の同一性の確認を行うようにすることができる。

【００３２】

また、より高いセキュリティが必要な各種情報に関しては、上記認証処理が成功した後に所望の情報格納ファイルにアクセスを許容するようにしたので、使い勝手を大幅に向上させながら、既存のユーザのプロファイル格納手法と同等のセキュリティレベルを確保することができる。

【００３３】

（第２の実施形態）

上記実施形態においては、階層的に構成される個別ファイル毎に独立した認証鍵が付与可能な記憶媒体の例として、ＩＣカードを利用した例を示した。この他にも、携帯端末機器等、他の記憶媒体に本発明を適用することができる。

【００３４】

また、利用者が携帯可能な、階層的に構成される個別ファイル毎に独立した認証鍵が付与可能な記憶機能を持つ機器との組み合わせる場合にも良好に利用することができる。

【００３５】

図６は、上述したユーザプロファイルの記憶方法及び装置を実現するコンピュータシステムの一例を示す図である。図６において、１２００はコンピュータＰＣである。ＰＣ１２００は、ＣＰＵ１２０１を備え、ＲＯＭ１２０２またはハードディスク（ＨＤ）１２１１に記憶された、あるいはフロッピーディスクドライブ（ＦＤ）１２１２より供給される制御ソフトウェアを実行し、システムバス１２０４に接続される各デバイスを総括的に制御する。上記ＰＣ１２００のＣＰＵ１２０１、ＲＯＭ１２０２またはハードディスク（ＨＤ）１２１１に記憶されたプログラムにより、本実施形態の各処理が実行される。

【００３６】

１２０３はＲＡＭで、ＣＰＵ１２０１の主メモリ、ワークエリア等として機能

する。１２０５はキーボードコントローラ（ＫＢＣ）で、キーボード（ＫＢ）１２０９等からの入力を制御する。

【００３７】

１２０６はＣＲＴコントローラ（ＣＲＴＣ）で、ＣＲＴディスプレイ（ＣＲＴ）１２１０の表示を制御する。１２０７はディスクコントローラ（ＤＫＣ）で、ブートプログラム（起動プログラム：パソコンのハードやソフトの実行（動作）を開始するプログラム）、複数のアプリケーション、ユーザファイルそしてネットワーク管理プログラム等を記憶するハードディスク（ＨＤ）１２１１、及びフロッピーディスク（ＦＤ）１２１２とのアクセスを制御する。

【００３８】

１２０８はネットワークインタフエースカード（ＮＩＣ）で、ＬＡＮ１２２０を介して、ネットワークプリンタ、他のネットワーク機器、あるいは他のＰＣと双方向のデータのやり取りを行うものである。さらに、上述した実施形態におけるユーザプロファイルをスマートカード１１に書きこむものである。

【００３９】

（本発明の他の実施形態）

本発明は複数の機器（例えば、ホストコンピュータ、インタフェース機器、リーダ、プリンタ等）から構成されるシステムに適用しても１つの機器からなる装置に適用しても良い。

【００４０】

また、上述した実施の形態の機能を実現するように各種のデバイスを動作させるように、上記各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、上記実施の形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ（ＣＰＵあるいはＭＰＵ）に格納されたプログラムに従って上記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【００４１】

また、この場合、上記ソフトウェアのプログラムコード自体が上述した実施の形態の機能を実現することになり、そのプログラムコード自体、およびそのプロ

グラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記憶媒体は本発明を構成する。かかるプログラムコードを記憶する記憶媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【００４２】

また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施の形態で説明した機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等の共同して上述の実施の形態で示した機能が実現される場合にもかかるプログラムコードは本発明の実施の形態に含まれることは言うまでもない。

【００４３】

さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって上述した実施の形態の機能が実現される場合にも本発明に含まれる。

【００４４】

【発明の効果】

以上説明したように、本発明によれば、高レベルなセキュリティが要求されるユーザのプロファイルは深い階層の個別ファイルに記憶し、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルに記憶するようにしたので、ユーザインタフェースや使用言語等等のように、積極的な提示が要求されるユーザのプロファイルは、初期認証の成功前に端末装置側から読み出すことができる。これにより、初期認証の成功以前から、ユーザ所望の入出力インタフェースでの動作が可能となり、しかも高レベルなセキュリティが要求されるユーザのプロファイルのセキュリティを高レベルに確保することができる。

【００４５】

また、より高いレベルのセキュリティが必要な各種情報に関しては、上記認証処理が成功した後にアクセスを許容するようにして、既存のユーザプロファイル格納手法と同等の高いセキュリティレベルが確保することができる。

【図面の簡単な説明】

【図１】

第１の実施形態における公共情報端末にスマートカード（ＩＣカード）を利用するようにしたシステムの概念を示す図である。

【図２】

第１の実施形態におけるＩＣカード内の論理ファイル構成を示す図である。

【図３】

端末利用者とＩＣカードの所有者とが一致する際の初期シーケンスを説明する図である。

【図４】

端末利用者とＩＣカード所有者が一致しない際の初期シーケンスを示す図である。

【図５】

ＩＣカードを装着した時に端末側で行われる処理手順の概要を説明するフローチャートである。

【図６】

コンピュータシステムの構成例を示すブロック図である。

【符号の説明】

１１　スマートカード（ＩＣカード）

１２　公共情報端末

１３　通信ネットワーク

１４　自治体情報サーバー

２００　ＩＣカード内主ファイル

２０１　主ファイル用情報ファイル

２１０　利用者認証アプリケーション用個別ファイル

２１１　カード所有者基礎情報格納用情報ファイル

２１２　カード所有者用セキュリティＢＯＸアプリケーション用個別ファイル

２１３　高セキュリティユーザ情報格納用情報ファイル

２１４　電子マネー系個別ファイルアクセス用情報格納ファイル

２１５　医療系個別ファイルアクセス用情報格納ファイル

２２０　医療系アプリケーション用個別ファイル

２２１　医療系アプリケーション用情報ファイル

２２２　電子カルテアプリケーション用個別ファイル

２２３　電子カルテアプリケーション用情報ファイル

２２４　電子カルテアプリケーション用情報ファイル（病歴）

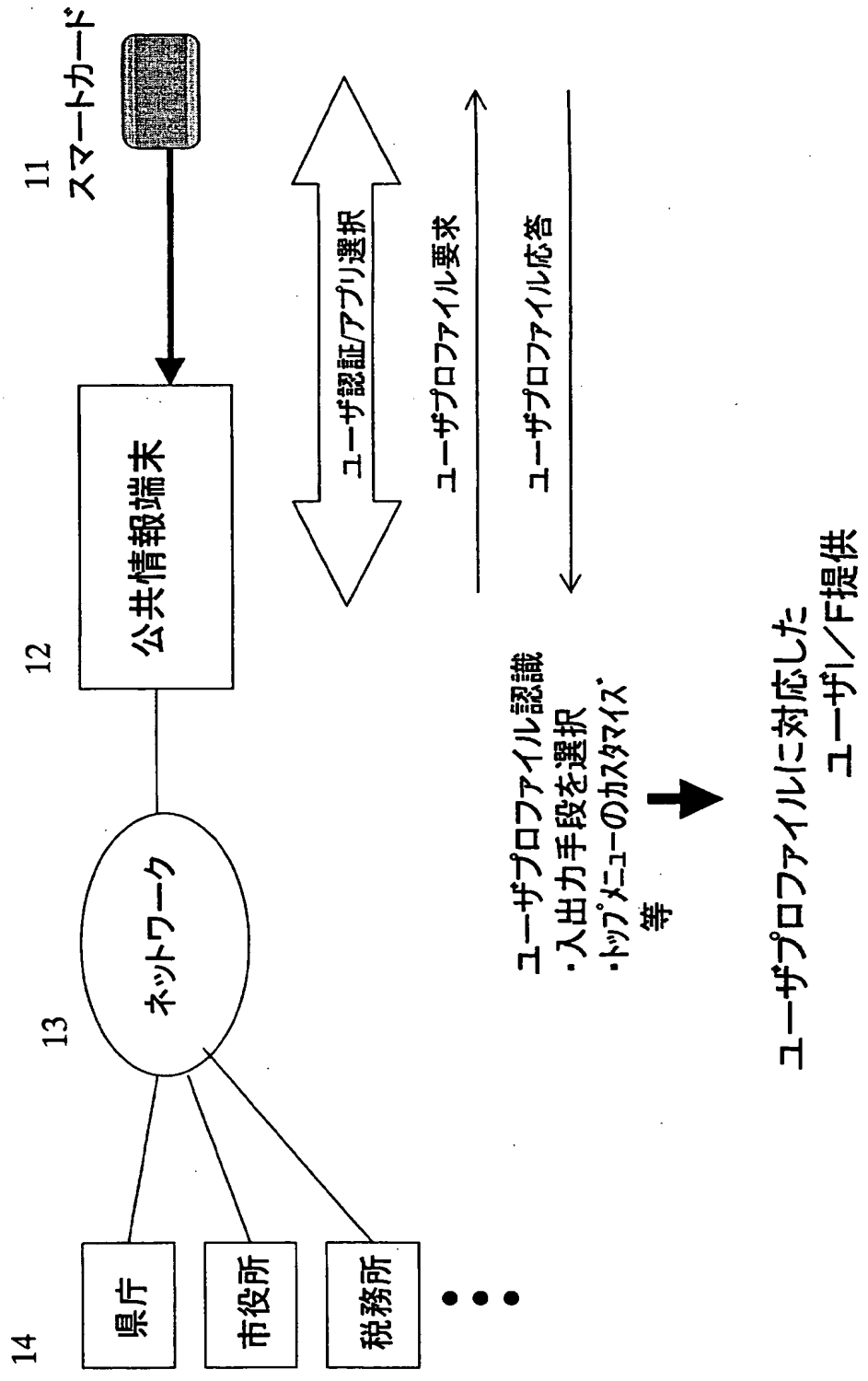
２３０　電子マネー系アプリケーション用個別ファイル

２３１　電子マネーアプリケーション用情報ファイル（取り引き履歴）

２３２　電子マネーアプリケーション用情報ファイル（残高）

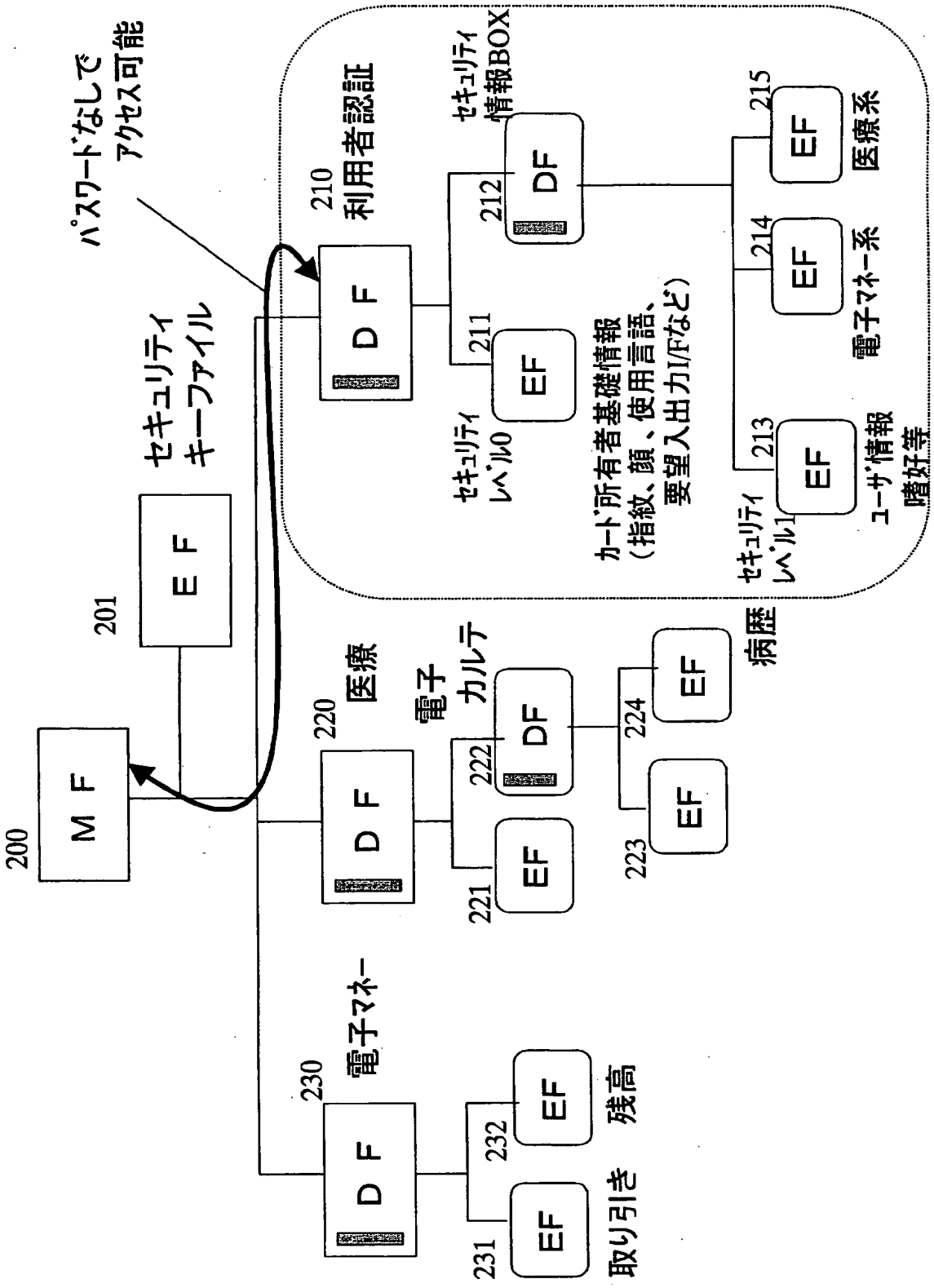
【書類名】　　図面

【図１】

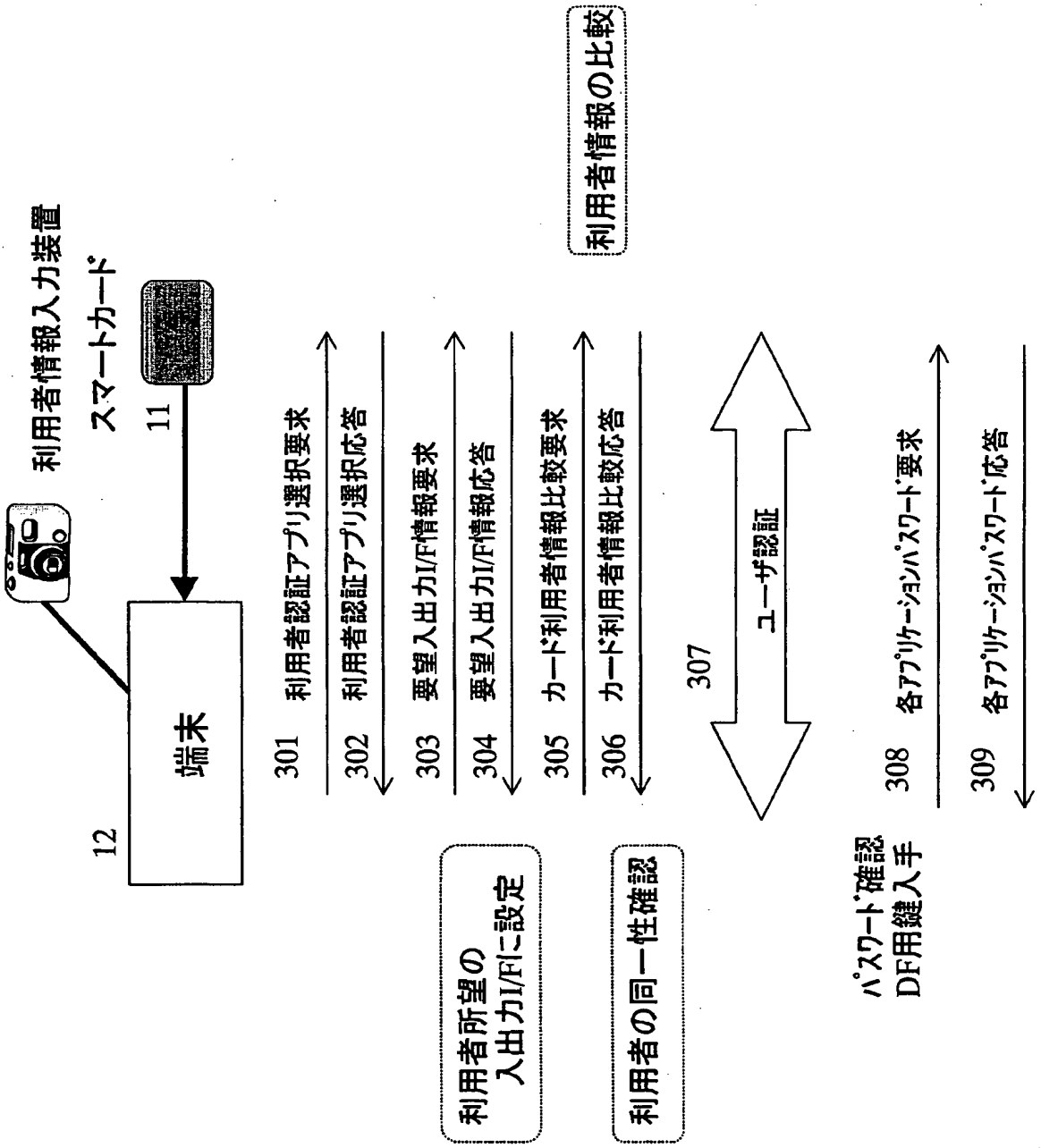


出証特２００１－３０４６９５９

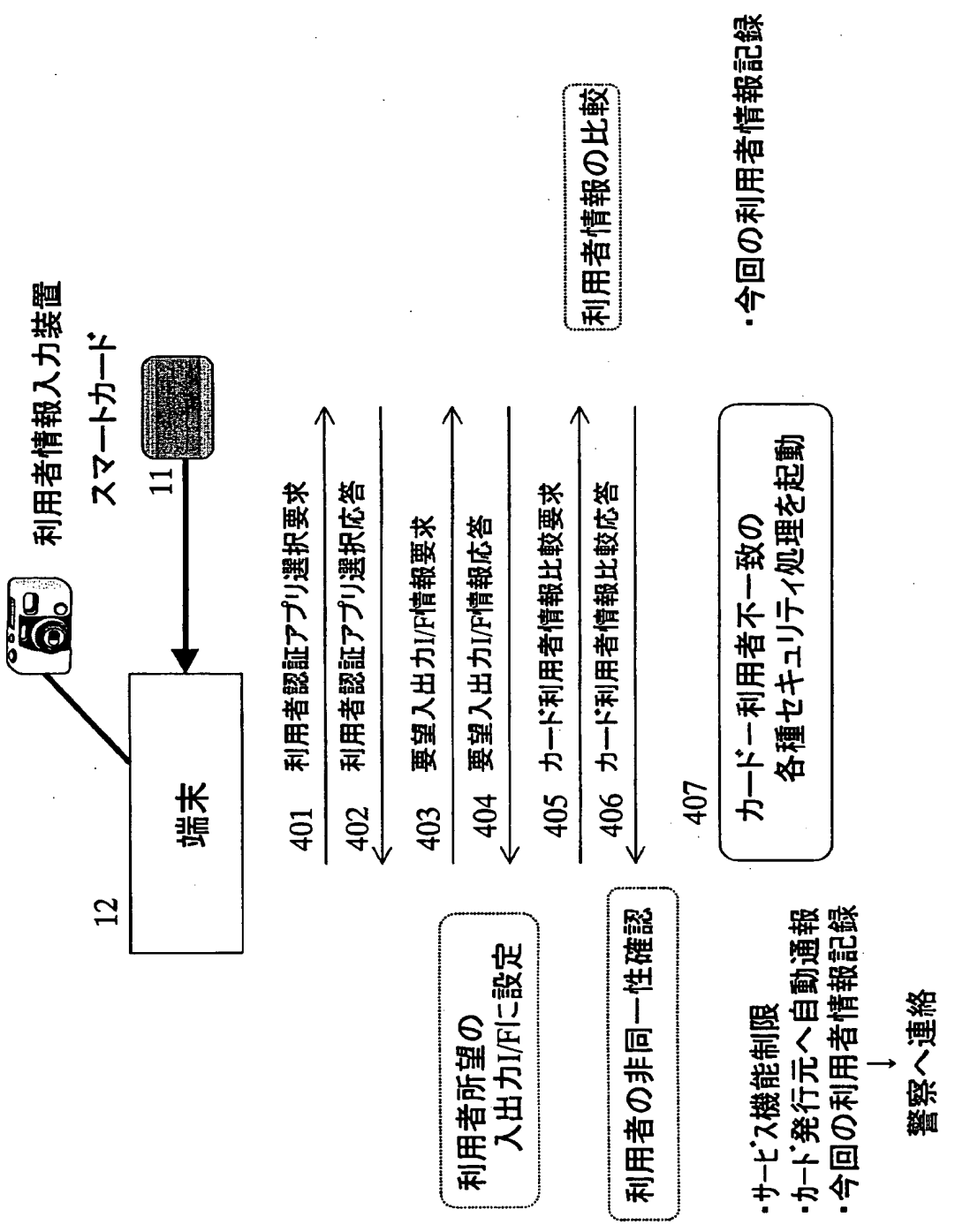
【図２】


パスワードなしで
アクセス可能
セキュリティ
キーファイル
200
MF
201
EF
210
利用者認証
DF
211
EF
セキュリティ
レベル0
カード所有者基礎情報
（指紋、顔、使用言語、
要望入出力I/Fなど）
212
DF
セキュリティ
情報BOX
213
EF
セキュリティ
レベル1
ユーザ情報
嗜好等
214
EF
電子マネー系
215
EF
医療系
220
DF
医療
電子
カルテ
221
EF
222
DF
223
EF
224
EF
病歴
230
DF
電子マネー
231
EF
232
EF
取り引き
残高

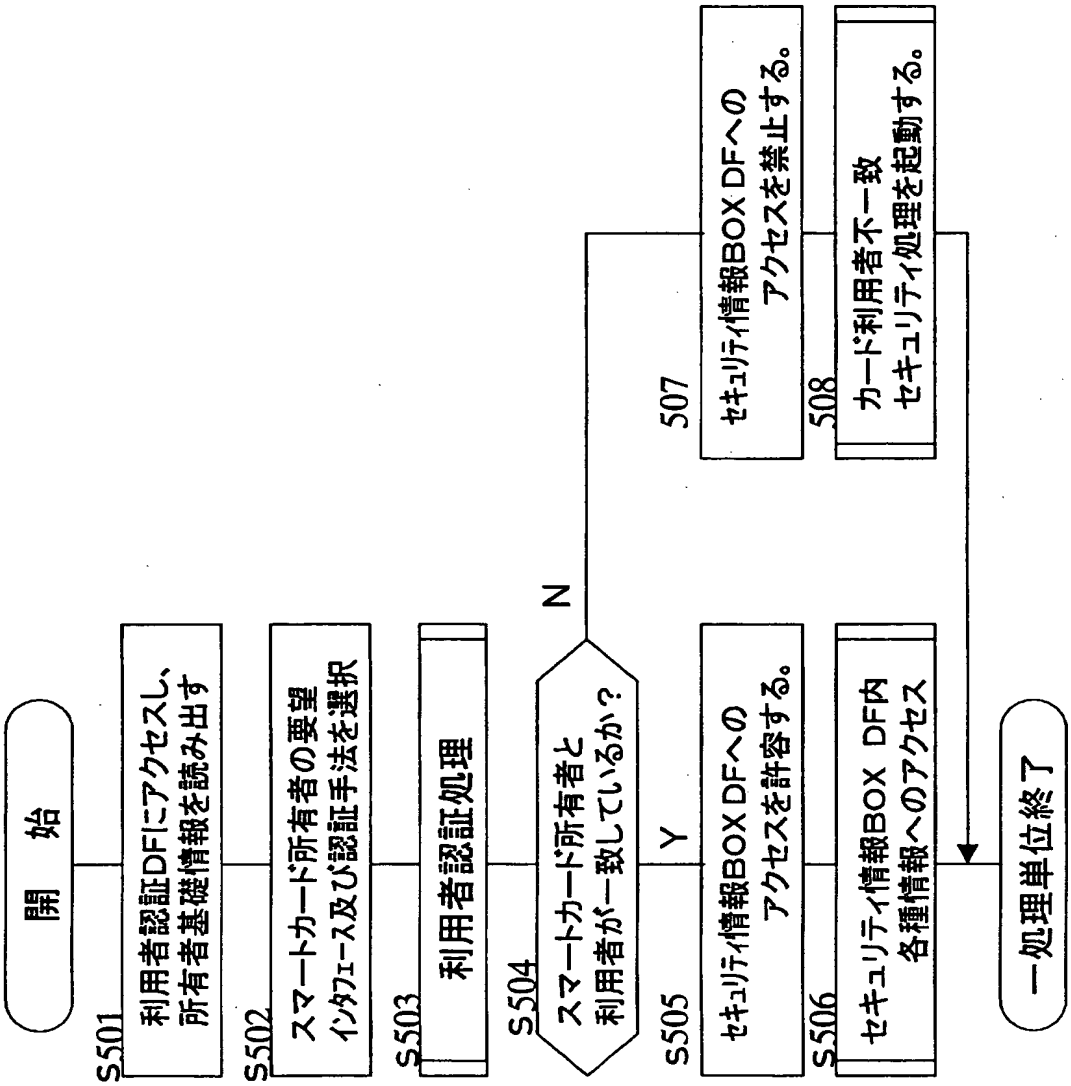
【図３】


利用者情報入力装置
スマートカード
11
12
端末
301 利用者認証アプリ選択要求
302 利用者認証アプリ選択応答
303 要望入出力I/F情報要求
304 要望入出力I/F情報応答
305 カード利用者情報比較要求
306 カード利用者情報比較応答
307
ユーザ認証
308 各アプリケーションパスワード要求
309 各アプリケーションパスワード応答
利用者情報の比較
利用者所望の
入出力I/Fに設定
利用者の同一性確認
パスワード確認
DF用鍵入手

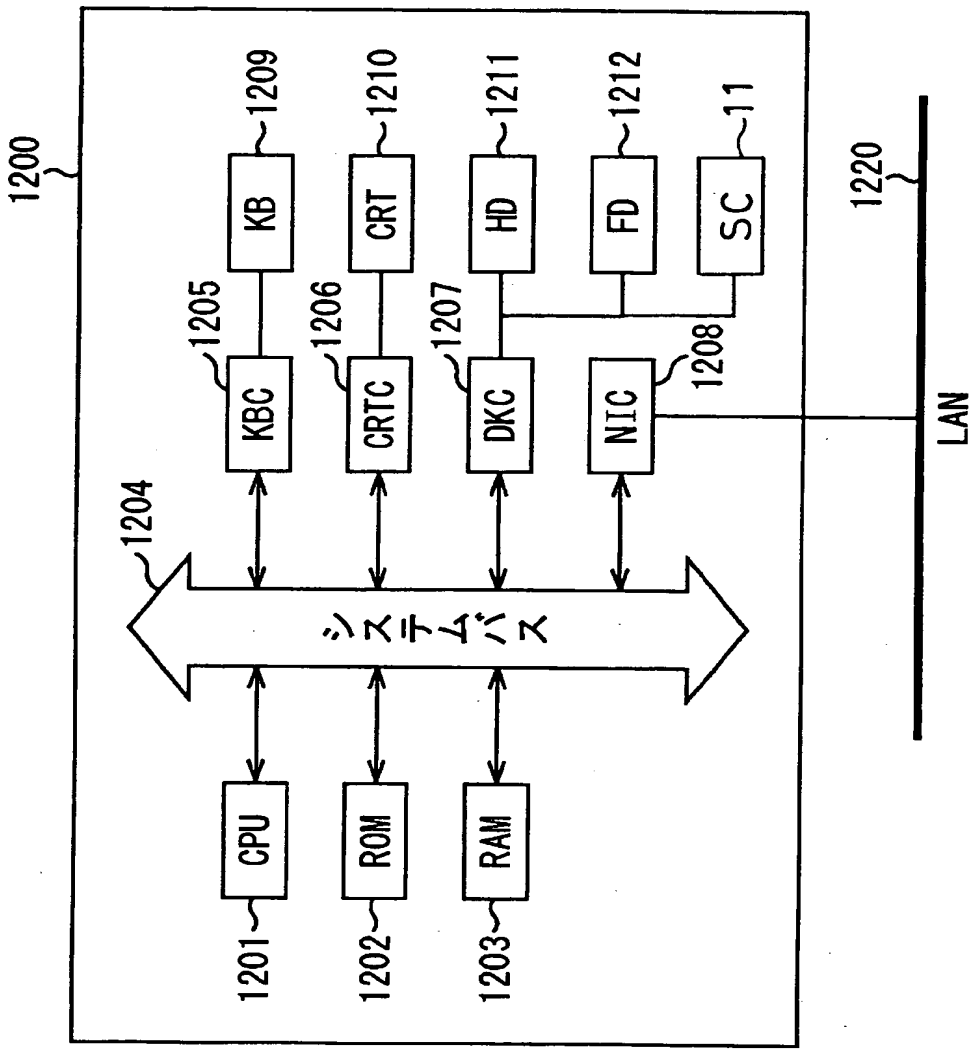
【図４】


利用者情報入力装置
スマートカード
11
12
端末
401 利用者認証アプリ選択要求
402 利用者認証アプリ選択応答
403 要望入出力I/F情報要求
404 要望入出力I/F情報応答
405 カード利用者情報比較要求
406 カード利用者情報比較応答
407
利用者情報の比較
・今回の利用者情報記録
利用者所望の
入出力I/Fに設定
利用者の非同一性確認
カード－利用者不一致の
各種セキュリティ処理を起動
・サービス機能制限
・カード発行元へ自動通報
・今回の利用者情報記録
→
警察へ連絡

【図５】


開　始
S501
利用者認証DFにアクセスし、所有者基礎情報を読み出す
S502
スマートカード所有者の要望インタフェース及び認証手法を選択
S503
利用者認証処理
S504
スマートカード所有者と利用者が一致しているか？
N
Y
S505
セキュリティ情報BOX DFへのアクセスを許容する。
S506
セキュリティ情報BOX DF内各種情報へのアクセス
507
セキュリティ情報BOX DFへのアクセスを禁止する。
508
カード利用者不一致セキュリティ処理を起動する。
一処理単位終了

【図６】


1200
1209
KB
1210
CRT
1211
HD
1212
FD
11
SC
1220
1205
KBC
1206
CRTC
1207
DKC
1208
NIC
LAN
1204
システムバス
CPU
ROM
RAM
1201
1202
1203

【書類名】　　要約書

【要約】

【課題】　高レベルなセキュリティが要求されるユーザのプロファイルを確実に保護した上で、ユーザが所望する入出力インタフェースを使用した情報の送受信を行うことができるようにする。

【解決手段】　ユーザのプロファイルを記憶するための個別ファイルを記憶媒体に階層的に複数層分用意し、高レベルなセキュリティが要求されるユーザのプロファイルは深い階層の個別ファイルに記憶し、積極的な提示が要求されるユーザのプロファイルは浅い階層の個別ファイルに記憶することにより、初期認証の成功以前から、ユーザ所望の入出力インタフェースでの動作を可能とし、かつ高レベルなセキュリティが要求されるユーザのプロファイルのセキュリティを高レベルに確保できるようにする。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００１００７〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都大田区下丸子３丁目３０番２号
氏　名　　キヤノン株式会社